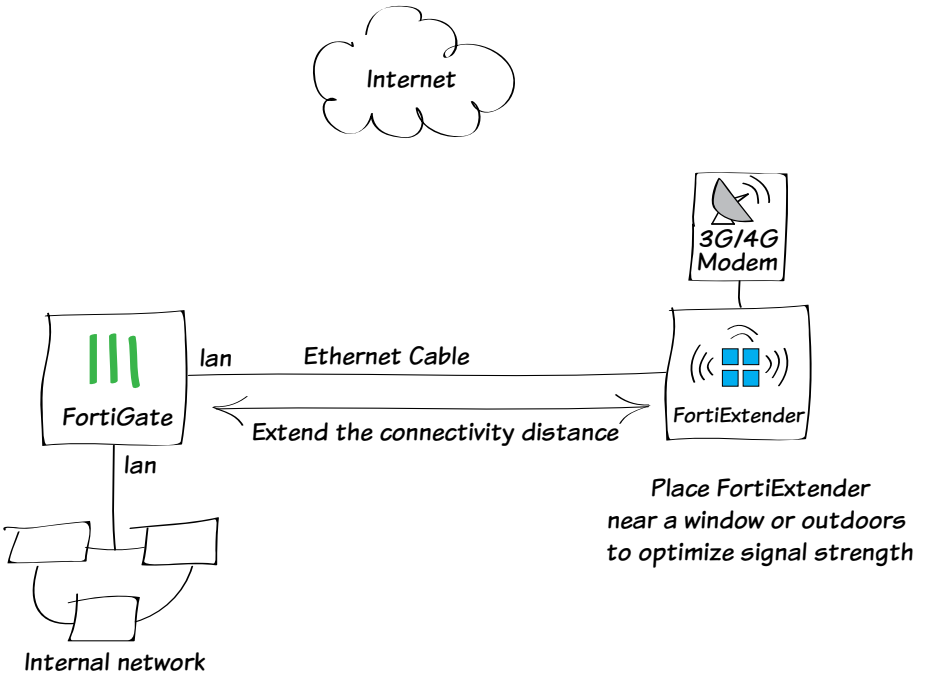
Setting up an Internet connection through a FortiGate unit using a 3G/4G modem and a FortiExtender

This example shows how to set an internet connection using a 3G/4G modem and a FortiExtender. A FortiExtender is used when the FortiGate unit is located in an area without 3G/4G network coverage, the FortiExtender can be placed near a window or outdoors.

1. Installing the 3G/4G modem in the FortiExtender
2. Connecting the FortiExtender
3. Configuring the FortiExtender
4. Modem settings
5. Configuring the FortiGate
6. Results



1. Installing the 3G/4G modem in the FortiExtender

Remove the housing cover of the FortiExtender and use the provided USB extension cable to connect your 3G/4G modem to the device.

For more information on installing the 3G/4G modem, see the QuickStart Guide.

2. Connecting the FortiExtender

Use an Ethernet cable to connect the FortiExtender to the **lan** interface of a FortiGate unit.

Once connected, FortiGate can control FortiExtender and modem.

Enable FortiExtender in the FortiGate's CLI

```
config system global
    set fortiextender enable
    set wireless-controller enable
end

config system interface
    edit lan
    set allowaccess capwap
end
```

CAPWAP service must be enabled on the port to which FortiExtender is connected, **lan** interface in this example.

Once enabled, it appears as a virtual WAN interface in the FortiGate, such as **fext-wan1**. Go to **System > Network > Interface** to verify **fext-wan1** interface.

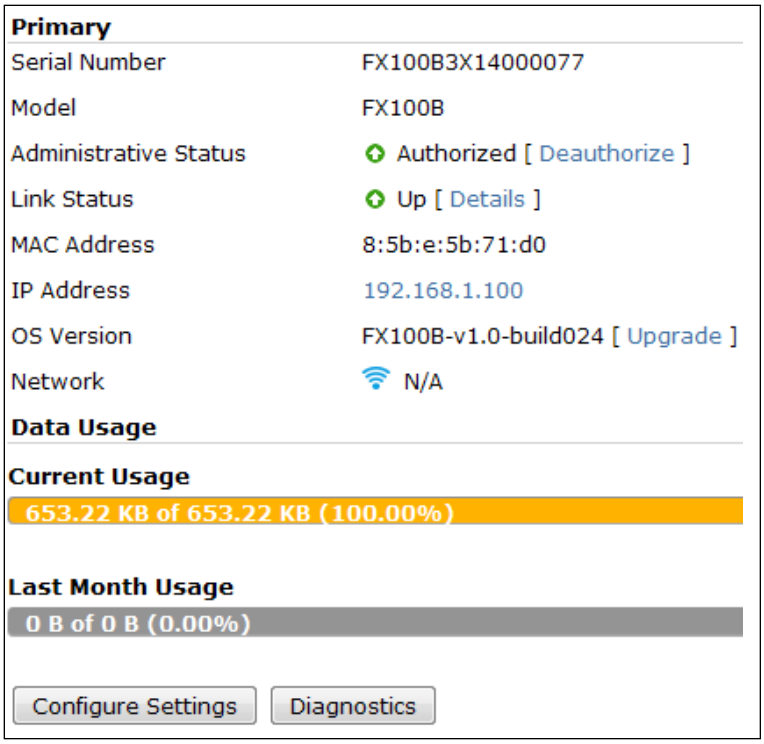
lan	Hardware Switch (16)
fext-wan1	FortiExtender

3. Configuring the FortiExtender

Go to **System > Network > FortiExtender** and authorize the FortiExtender.

Primary	
Serial Number	FX100B3X14000077
Administrative Status	Deauthorized [Authorize]

Once authorized, you can see the status of the FortiExtender.

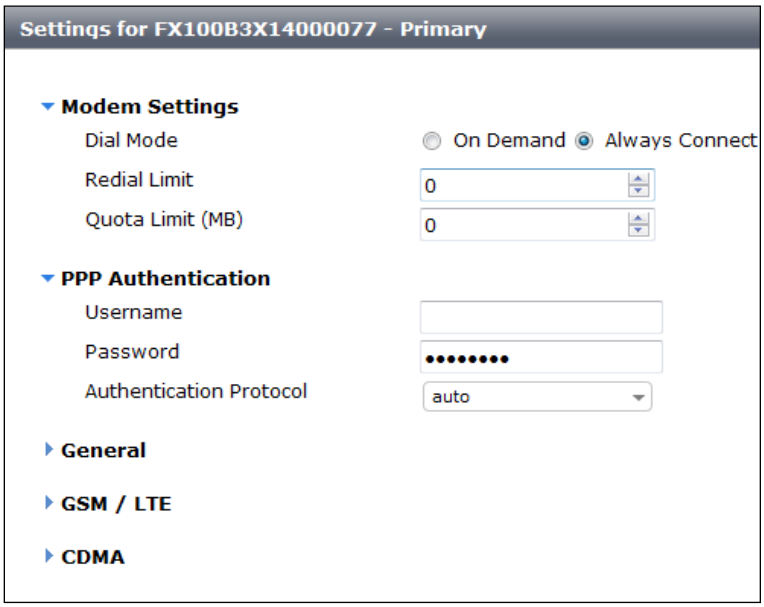


4. Modem settings

The FortiExtender unit allows for two modes of operation for the modem; On Demand and Always Connect.

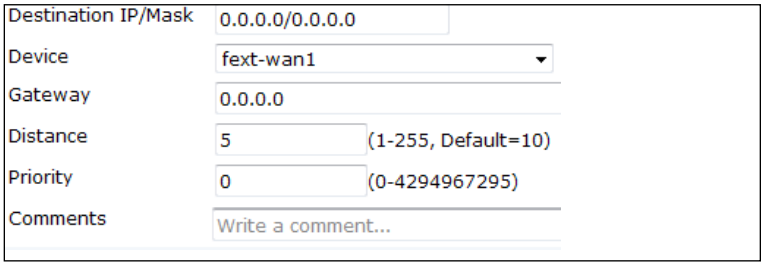
Go to **System > Network > FortiExtender** and click on **Configuring Settings**.

Select **Always Connect** for **Dial Mode** and keep other settings to default.

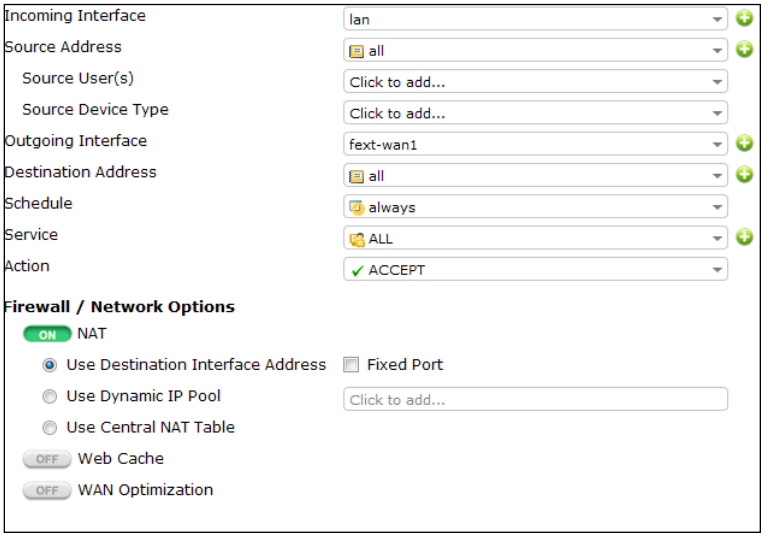


5. Configuring the FortiGate

Go to **Router > Static > Static Routes** and add new route through **fext-wan1** interface.

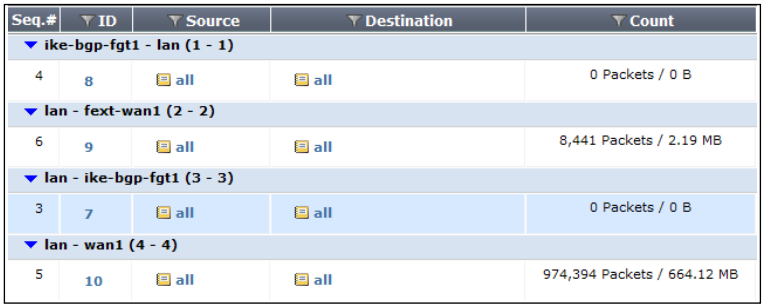


Go to **Policy & Objects > Policy > IPv4** and create a new security policy allowing traffic from **lan** interface to **fext-wan1** interface.



6. Results

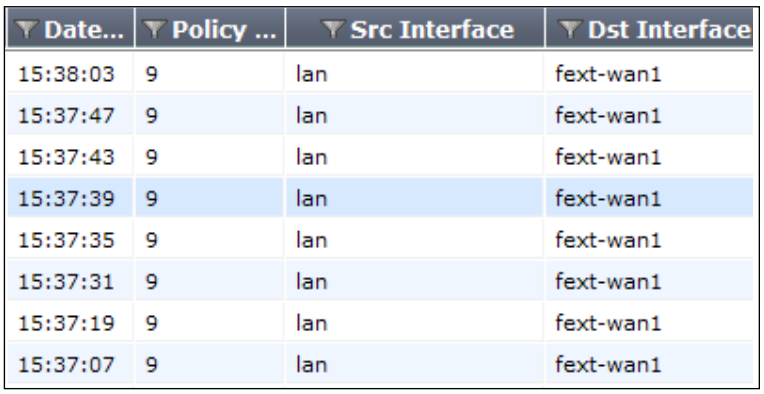
Browse the Internet and go to **Policy & Objects > Policy > IPv4** to verify the **Count**.



Seq.#	ID	Source	Destination	Count
ike-bgp-fgt1 - lan (1 - 1)				
4	8	all	all	0 Packets / 0 B
lan - fext-wan1 (2 - 2)				
6	9	all	all	8,441 Packets / 2.19 MB
lan - ike-bgp-fgt1 (3 - 3)				
3	7	all	all	0 Packets / 0 B
lan - wan1 (4 - 4)				
5	10	all	all	974,394 Packets / 664.12 MB

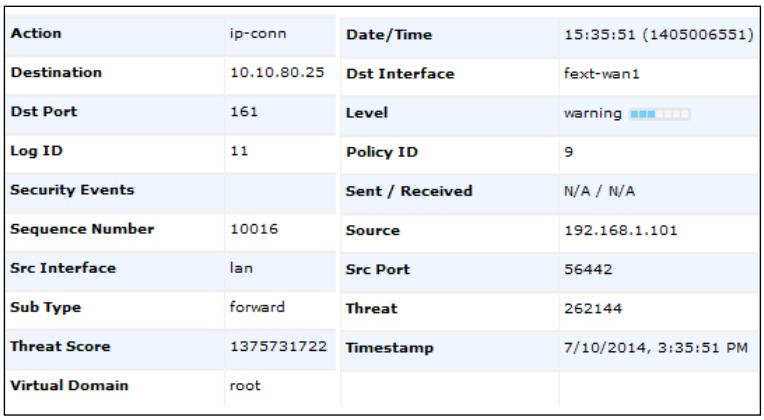
Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic flowing from **lan** interface to **fext-wan1** interface.



Date...	Policy ...	Src Interface	Dst Interface
15:38:03	9	lan	fext-wan1
15:37:47	9	lan	fext-wan1
15:37:43	9	lan	fext-wan1
15:37:39	9	lan	fext-wan1
15:37:35	9	lan	fext-wan1
15:37:31	9	lan	fext-wan1
15:37:19	9	lan	fext-wan1
15:37:07	9	lan	fext-wan1

Select an entry for details



Action	ip-conn	**Date/Time**	15:35:51 (1405006551)
Destination	10.10.80.25	**Dst Interface**	fext-wan1
Dst Port	161	**Level**	warning
Log ID	11	**Policy ID**	9
Security Events		**Sent / Received**	N/A / N/A
Sequence Number	10016	**Source**	192.168.1.101
Src Interface	lan	**Src Port**	56442
Sub Type	forward	**Threat**	262144
Threat Score	1375731722	**Timestamp**	7/10/2014, 3:35:51 PM
Virtual Domain	root		